FY2010 FISMA Benchmark Metrics

Major & Small Agencies

- *All estimates should be based on a random and statistically significant sample.*
- *Metrics marked with an asterisk (*) will be asked on a quarterly (not annual) basis and will fulfill the agency FY2009 Q4 report submission requirement. The Q4 questions must be answered at the same time for the FY2010 annual submission to be considered "complete" by the CyberScope system.*
- *Questions labeled as "Data Feeds" will be required for all Major (CFO Act) Agencies and optional for all Small Agencies.*

System Inventory

1. For each of the subparts in this question, provide the total number of Agency operational systems (both Agency operated and contractor operated) by Agency component (i.e. Bureau or Major Operating Element).

   This question will be answered by subcomponent.

   a. Number of "low" category systems.
   b. Number of "medium" category systems.
   c. Number of "high" category systems.
   d. Number of systems with a current authorization to operate.

Asset Management

2. Provide the estimated total number of Agency Information Technology assets (e.g. router, server, workstation, laptop, blackberry, etc.). *Responses to this question will be used as a denominator in calculating agency benchmarks as a percentage.*

   a. Provide the estimated number of Agency information technology assets (e.g. router, server, workstation, laptop, blackberry, etc.) where an automated capability provides visibility at the Agency level into detailed asset inventory information.
   b. Provide the estimated number of Agency information technology assets where all of the following asset inventory information is collected: Network address, Machine Name, Operating System, and Operating System/Patch Level.

3. What is the estimated average percentage of assets for which inventory information could be collected at the Agency level within a 48 hour time period?

   DATA FEED: For the estimated number of Agency information technology assets where an automated capability provides visibility at the Agency level into the asset inventory information, upload the list of operating systems in use providing the vendor, product, and version of each operating system as a set of Common Platform Enumeration (CPE) names and include the number of assets running each listed operating system.

Configuration Management

4. Provide the estimated number of Agency information technology assets where an automated capability provides visibility at the Agency level into asset system configuration information (e.g. comparison of agency baselines to installed configurations).

5. *For each type of operating system software in use across the Agency, provide the percentage for which standard security configuration baselines are defined. *It is understood that this metric does not include the number of instances of each OS across the agency; therefore, this metric does not directly reflect the amount of risk for an Agency as very few OS's could and likely do cover the majority of assets. This question will be answered by subcomponent.*

   EXAMPLE: A given Agency has 115 different operating systems in use across their various components to include legacy applications, etc. Of those 115, the Agency has defined and approved standard security baseline settings for 75 of them. The answer to this question, therefore, would be 75/115 = 65%.

6. Upload the listing of deviations between Agency subcomponent approved security configuration baselines and FDCC/USGCB baselines. Deviations should be reported by Common Configuration Enumeration (CCE) ID.

   DATA FEED: For Agency information technology assets where an automated capability provides visibility at the Agency level into detailed asset configuration information, upload the listing of deviations from the Agency subcomponent approved security configuration baselines including the number of systems with each reported deviation. Deviations should be reported by Common Configuration Enumeration (CCE) ID.

Vulnerability Management

7. Provide the estimated number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (e.g. Common Vulnerability Enumerations).

   DATA FEED: For Agency information technology assets where an automated capability provides visibility at the Agency level into detailed asset vulnerability information, provide the average number of open vulnerabilities per asset across the Agency with a CVSS base score (as provided in the National Vulnerability Database) equal to or higher than 7.0, including the number of systems affected by each vulnerability.

Identity and Access Management

8. Provide a working URL to the Agency’s progress update for HSPD-12 implementation.

9. What is the estimated number of Agency network user accounts? *This metric will be used as the denominator in several Training and Education questions.*

10. What estimated number of Agency network user accounts are configured to require PIV credentials to authenticate to the Agency network(s)?

Data Protection

11. Provide the estimated number of:
    a. Portable computers (i.e. laptops).
    b. Those portable computers in (a) that have all user data encrypted with FIPS 140-2 validated encryption.

Network Security Protocols

12. *Provide the number of:
    a. *DNS names (second-level).
    b. *DNS names (second-level) signed.

13. *Provide the percentage of DNS hierarchies with all sub-domains (second-level and below) entirely signed.

Boundary Protection

14. Provide the percentage of the required TIC 1.0 Capabilities implemented. *This question applies to Federal Civilian Agency TIC Access Providers (TICAPs) only. All others should respond with "N/A."*

15. Provide the percentage of TICs with operational NCPS (Einstein 2) deployment. *This question applies to Federal Civilian Agency TIC Access Providers (TICAPs) only. All others should respond with "N/A."*

16. Provide the percentage of external network capacity passing through a TIC/MTIPS. *This question applies to Federal Civilian Agency only. All others should respond with "N/A."*

17. Provide the percentage of external connections passing through a TIC/MTIPS. *This question applies to Federal Civilian Agency only. All others should respond with "N/A."*

18. *Provide the percentage of agency email systems that implement sender verification (anti-spoofing) technologies when sending messages to government agencies or the public such as S/MIME, HSPD-12, PGP, DKIM, and SPF.
    a. *List the technologies from (a) currently in use.

19. *Provide the percentage of agency email systems that check sender verification (anti-spoofing technologies) to detect possibly forged messages from government agencies known to send email with sender verification such as S/MIME, PGP, DKIM or SPF.
    a. *List the technologies from (a) currently in use.

Incident Management

20. What is the estimated number of Agency operational networks on which controlled network penetration testing was performed in the past year? *Penetration Testing is defined as test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. Network penetration testing is penetration testing performed on the Agency network.*

21. For the networks counted above, provide the following estimated information:
    a. Percentage of incidents detected by NOC/SOC.
    b. Mean-time to incident detection.
    c. Mean-time to incident remediation.
    d. Mean-time to incident recovery.

22. For FY10, what percentage of U.S. CERT SARs (or Information Assurance Vulnerability Alerts for DOD) has been remediated by the Agency? *For this estimate, do not include the Monthly Watch List in the Agency calculation. The current list of SARS is on the GFIRST portal.*

23. What is the mean-time between incident detection and incident reporting to US-CERT (or DoD equivalent)?

Training and Education

24. What is the average frequency that users receive supplemental cybersecurity awareness training content beyond the annual training requirement (content could include a single question or tip of the day)? *This question will be answered by subcomponent.*

25. Provide the number of Agency users with log-in privileges that have been given security awareness training annually.

26. Provide the number of Agency users with significant security responsibilities.
    a. Provide the number of Agency users with significant security responsibilities that have been given specialized, role based, security training annually.

27. At what frequency is security awareness training content (that is provided to users) updated by the Agency or training provider?

28. At what frequency is specialized, role based, security training content (that is provided to users) updated by the Agency?

29. Provide the percentage of positions with significant security responsibilities that are filled with security certified personnel. *This question is to be answered by the Department of Defense only. All other agencies should choose "N/A".*

30. Provide the estimated percentage of new users to satisfactorily complete security awareness training before being granted network access.

Remote Access / Telework

The following questions refer to connection methods the Agency offers to allow users to connect remotely (i.e. Dial-Up, VPN, Clientless-VPN or SSL, WiFi, Wireless/Cellular, etc). All estimates should be based on a random and statistically significant sample.

31. Provide the estimated number of remote access connection methods (connection methods the Agency offers to allow users to connect remotely such as Dial-Up, VPN, Clientless-VPN or SSL, WiFi, Wireless/Cellular, etc.) to Agency LAN/WAN resources/services.

32. For those methods provided above, provide the number that:
    a. Require only password.
    b. Require only PIV credentials.
    c. Require other forms of two-factor authentication.
    d. Utilize FIPS 140-2 validated cryptographic modules.
    e. Require Government Furnished Equipment (GFE).
    f. Assess and correct system configuration upon connection.
    g. Scan for viruses and malware upon connection.
    h. Prohibit split tunneling.
    i. Are configured to time-out after 15 minutes of inactivity requiring re-authentication.